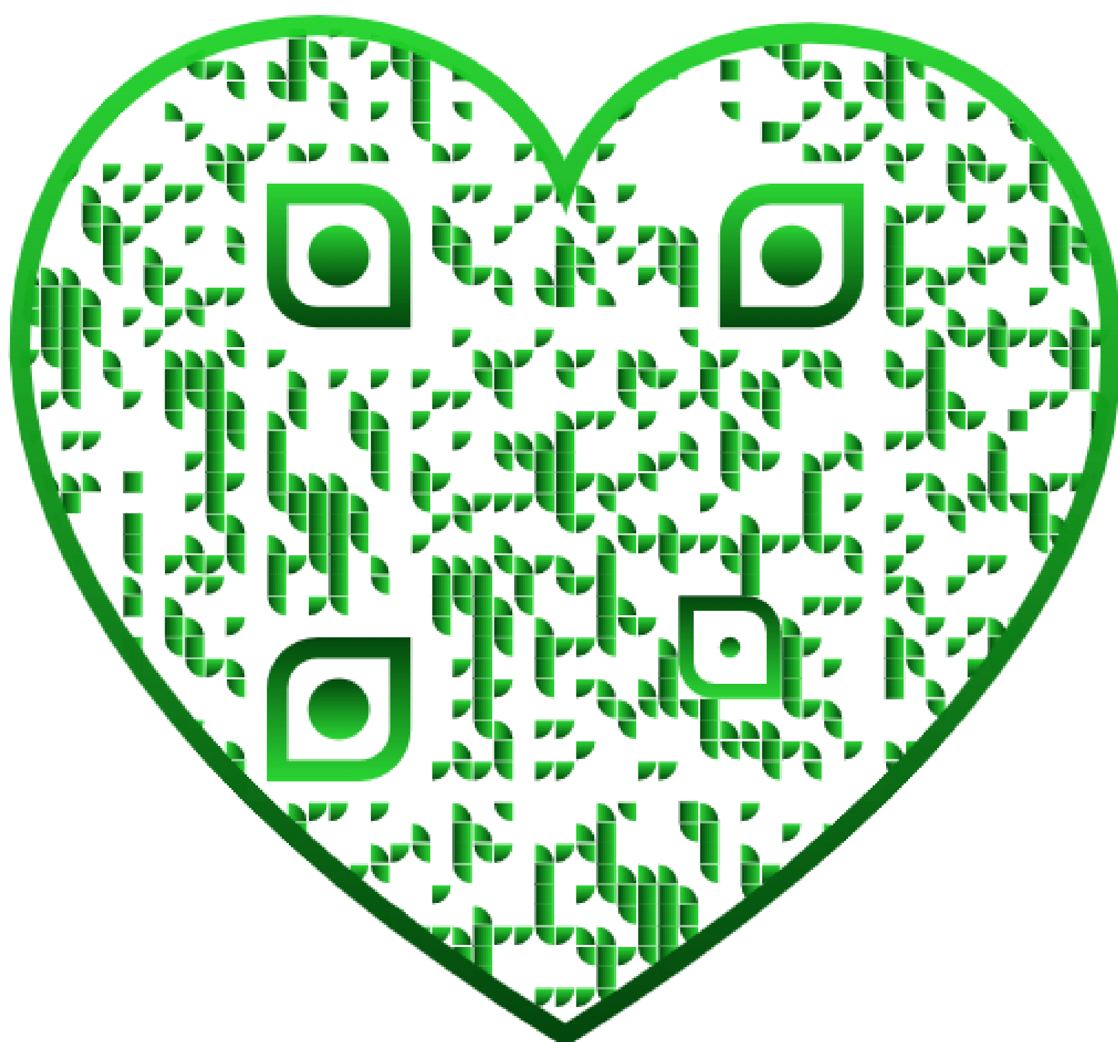
LIBERDADE E O FUTURO DA INTERNET

CYPHERPUNKS

JULIAN ASSANGE

COM JACOB APPELBAUM, ANDY MÜLLER-MAGUHN E JÉRÉMIE ZIMMERMANN

BOITEMPO EDITORIAL



**** SYSTEM FAILURE ***



Capa da edição de 13 dez. 2010 da revista norte-americana *Time*, com matérias sobre Julian Assange e o WikiLeaks.

LIBERDADE E O FUTURO DA INTERNET

CYPHERPUNKS

JULIAN ASSANGE

COM **JACOB APPELBAUM, ANDY MÜLLER-MAGUHN E JÉRÉMIE ZIMMERMANN**

TRADUÇÃO **CRISTINA YAMAGAMI**

BOITEMPO
EDITORIAL

Copyright © Julian Assange, 2012
Copyright desta tradução © Boitempo Editorial, 2013
Traduzido do original em inglês *Cypherpunks: freedom and the future of the internet*
publicado nos Estados Unidos pela OR Books LLC, Nova York

Coordenação editorial
Ivana Jinkings

Editora-adjunta
Bibiana Leme

Assistência editorial
Alícia Toffani e Livia Campos

Tradução
Cristina Yamagami

Consultoria técnica
Pablo Ortellado

Preparação
Thaisa Burani

Capa e guardas
Ronaldo Alves Filho
sobre imagem do vídeo "Collateral Murder"
(foto de Julian Assange na quarta capa: Allen Clark)

Diagramação
Crayon Editorial

Produção
Livia Campos

É vedada a reprodução de qualquer
parte deste livro sem a expressa autorização da editora.

CIP-BRASIL. CATALOGAÇÃO-NA-FONTE
SINDICATO NACIONAL DOS EDITORES DE LIVROS, RJ

C996
Cypherpunks : liberdade e o futuro da internet / Julian Assange ... [et al.] ; tradução Cristina Yamagami. - São Paulo : Boitempo, 2013.
Tradução de: Cypherpunks: freedom and the future of the internet
ISBN 978-85-7559-307-3

1. WikiLeaks 2. Política internacional 3. Política econômica 4. Internet - Aspectos sociais. I. Assange, Julian, 1971-.

13-0102. CDD: 327
CDU: 327
07.01.13 08.01.13 041946

Este livro atende às normas do acordo ortográfico em vigor desde janeiro de 2009.

1ª edição: fevereiro de 2013

BOITEMPO EDITORIAL
Jinkings Editores Associados Ltda.
Rua Pereira Leite, 373
05442-000 São Paulo SP
Tel./fax: (11) 3875-7250 / 3872-6869
editor@boitempoeditorial.com.br
www.boitempoeditorial.com.br

O que é um cypherpunk?

Os cypherpunks defendem a utilização da criptografia e de métodos similares como meio para provocar mudanças sociais e políticas[1]. Criado no início dos anos 1990, o movimento atingiu seu auge durante as "criptoguerras" e após a censura da internet em 2011, na Primavera Árabe. O termo *cypherpunk* – derivação (criptográfica) de *cipher* (escrita cifrada) e *punk* – foi incluído no *Oxford English Dictionary* em 2006[2].

1 De maneira simplificada, a palavra "criptografia" tem origem no termo grego para "escrita secreta" e designa a prática de se comunicar em código.

2 "Oxford English Dictionary Updates Some Entries & Adds New Words; Bada-Bing, Cypherpunk, and Wi-Fi Now in the OED", *ResourceShelf*, 16 set. 2006, disponível em: <http://web.resourceshelf.com/go/resourceblog/43743>. Acesso em 24 out. 2012.

Nota da edição

Esta edição de *Cypherpunks – liberdade e o futuro da internet*, a primeira a ser lançada na América Latina, vem acrescida de um prefácio especial de Julian Assange, inédito até sua publicação no Brasil.

Tendo por base uma conversa entre os quatro autores, o texto foi depois reelaborado por eles a fim de esclarecer passagens que poderiam soar confusas. Também foram acrescidas notas explicativas em pontos-chave, porém a ordem do manuscrito, em geral, é a mesma do diálogo original.

Nesta tradução, optou-se por verter os termos "whistleblowing" e "whistleblower" para "denúncia" e "denunciante", respectivamente. Ainda sem tradução consensual na área do jornalismo investigativo brasileiro, os termos fazem referência a membros de organizações, empresas ou governos que denunciam por livre e espontânea vontade as mazelas do sistema na esperança de que elas sejam solucionadas.

O termo "cypherpunk", por sua vez, pode ser traduzido em português como "criptopunk" (ver explicação na p. anterior). Não obstante, optou-se nesta edição por mantê-lo em sua forma original, internacionalmente utilizada, em razão das ligações estabelecidas no texto com o movimento Cypherpunk e a lista de discussões on-line de mesmo nome.

Agradecemos a colaboração da jornalista Natalia Viana, na elaboração da apresentação à edição brasileira, e do professor da Escola de Artes, Ciências e Humanidades da Universidade de São Paulo Pablo Ortellado, na consultoria técnica desta edição.

Sumário

Apresentação: O WikiLeaks e as batalhas digitais de Julian Assange – *Natalia Viana* ... 9

Prefácio para a América Latina – *Julian Assange* ... 19

Introdução: Um chamado à luta criptográfica – *Julian Assange* ... 25

Os autores ... 31

1. Observações sobre as várias tentativas de perseguição ao WikiLeaks e às pessoas a ele associadas ... 37
2. Maior comunicação *versus* maior vigilância ... 43
3. A militarização do ciberespaço ... 53
4. Combatendo a vigilância total com as leis do homem ... 63
5. Espionagem pelo setor privado ... 71
6. Combatendo a vigilância total com as leis da física ... 79
7. Internet e política ... 85
8. Internet e economia ... 101
9. Censura ... 121
10. Privacidade para os fracos, transparência para os poderosos ... 143
11. Ratos na ópera ... 149

Cronologia WikiLeaks ... 159

Prefácio para a América Latina

A luta do WikiLeaks é uma luta de muitas facetas. Em meu trabalho como jornalista, lutei contra guerras e para forçar os grupos poderosos a prestarem contas ao povo. Em muitas ocasiões, manifestei-me contra a tirania do imperialismo, que hoje sobrevive no domínio econômico-militar da superpotência global.

Por meio desse trabalho, aprendi a dinâmica da ordem internacional e a lógica do império. Vi países pequenos sendo oprimidos e dominados por países maiores ou infiltrados por empreendimentos estrangeiros e forçados a agir contra os próprios interesses. Vi povos cuja expressão de seus desejos lhes foi tolhida, eleições compradas e vendidas, as riquezas de países como o Quênia sendo roubadas e vendidas em leilão a plutocratas em Londres e Nova York. Expus grande parte disso, e continuarei a expor, apesar de ter me custado caro.

Essas experiências embasaram minha atuação como um cypherpunk. Elas me deram uma perspectiva sobre as questões discutidas nesta obra, que são de especial interesse para os leitores da América Latina. O livro não explora essas questões a fundo. Para isso seria necessário outro – muitos outros livros. Mas quero chamar a atenção para essas questões e peço que você as mantenha em mente durante a leitura.

Os últimos anos viram o enfraquecimento das velhas hegemonias. Do Magrebe até o Golfo Pérsico, as populações têm combatido a tirania em defesa da liberdade e da autodeterminação. Movimentos populares no Paquistão e na Malásia acenam com a promessa de uma nova força no cenário mundial. E a América Latina tem visto o tão esperado despontar da soberania e da independência, depois de séculos de brutal dominação imperial. Esses avanços constituem a esperança do nosso mundo, enquanto o sol se põe na democracia no Primeiro Mundo. Vivenciei em primeira mão essa nova independência e vitalidade da América Latina quando o

Equador, o Brasil e a região se apresentaram em defesa dos meus direitos depois que recebi asilo político.

A longa luta pela autodeterminação latino-americana é importante por abrir o caminho para que o resto do mundo avance na direção da liberdade e da dignidade. Mas a independência latino-americana ainda está engatinhando. Os Estados Unidos ainda tentam subverter a democracia latino-americana em Honduras e na Venezuela, no Equador e no Paraguai. Nossos movimentos ainda são vulneráveis. É vital que eles tenham sucesso. Portanto, devem ser protegidos.

É por isso que a mensagem dos cypherpunks é de especial importância para o público latino-americano. O mundo deve se conscientizar da ameaça da vigilância para a América Latina e para o antigo Terceiro Mundo. A vigilância não constitui um problema apenas para a democracia e para a governança, mas também representa um problema geopolítico. A vigilância de uma população inteira por uma potência estrangeira naturalmente ameaça a soberania. Intervenção após intervenção nas questões da democracia latino-americana nos ensinaram a ser realistas. Sabemos que as antigas potências colonialistas usarão qualquer vantagem que tiverem para suprimir a independência latino-americana.

Este livro discute o que acontece quando corporações norte-americanas como o Facebook têm uma penetração praticamente completa na população de um país, mas não discute as questões geopolíticas mais profundas.

Um aspecto importante vem à tona se levamos em consideração as questões geográficas. Para tanto, a ideia do "exército ao redor de um poço de petróleo" é interessante. Todo mundo sabe que o petróleo orienta a geopolítica global. O fluxo de petróleo decide quem é dominante, quem é invadido e quem é excluído da comunidade global. O controle físico até mesmo de um segmento de oleoduto resulta em grande poder geopolítico. E os governos que se veem nessa posição são capazes de conseguir enormes concessões.

De tal forma que, em um só golpe, o Kremlin é capaz de condenar o Leste Europeu e a Alemanha a um inverno sem aquecimento. E até a perspectiva de Teerã abrir um oleoduto do Oriente até a Índia e a China é um pretexto para Washington manter uma lógica belicosa.

A mesma coisa acontece com os cabos de fibra óptica. A próxima grande alavanca no jogo geopolítico serão os dados resultantes da vigilância: a vida privada de milhões de inocentes.

Não é segredo algum que, na Internet, todos os caminhos que vão e vêm da América Latina passam pelos Estados Unidos. A infraestrutura da internet direciona a maior parte do tráfego que entra e sai da América do Sul por linhas de fibra óptica que cruzam fisicamente as fronteiras dos Estados Unidos. O governo norte-americano tem violado sem nenhum escrúpulo as próprias leis para mobilizar es-

sas linhas e espionar seus cidadãos. E não há leis contra espionar cidadãos estrangeiros. Todos os dias, centenas de milhões de mensagens vindas de todo o continente latino-americano são devoradas por órgãos de espionagem norte-americanos e armazenadas para sempre em depósitos do tamanho de cidades. Dessa forma, os fatos geográficos referentes à infraestrutura da internet têm consequências para a independência e a soberania da América Latina. Isso deve ser levado em consideração nos próximos anos, à medida que cada vez mais latino-americanos entrarem na internet.

O problema também transcende a geografia. Muitos governos e militares latino-americanos protegem seus segredos com hardware criptográfico. Esses hardwares e softwares embaralham as mensagens, desembaralhando-as quando chegam a seu destino. Os governos os compram para proteger seus segredos, muitas vezes com grandes despesas para o povo, por temerem, justificadamente, a interceptação de suas comunicações pelos Estados Unidos.

Mas as empresas que vendem esses dispendiosos dispositivos possuem vínculos estreitos com a comunidade de inteligência norte-americana. Seus CEOs e funcionários seniores são matemáticos e engenheiros da NSA, capitalizando as invenções que criaram para o Estado de vigilância. Com frequência seus dispositivos são deliberadamente falhos: falhos com um propósito. Não importa quem os está utilizando ou como – os órgãos de inteligência norte-americanos são capazes de decodificar o sinal e ler as mensagens.

Esses dispositivos são vendidos a países latino-americanos e de outras regiões que desejam proteger seus segredos, mas na verdade constituem uma maneira de roubar esses segredos. Os governos estariam mais seguros se usassem softwares criptográficos feitos por cypherpunks, cujo design é aberto para todos verem que não se trata de uma ferramenta de espionagem, disponibilizados pelo preço de uma conexão com a internet.

Enquanto isso, os Estados Unidos estão acelerando a próxima grande corrida armamentista. A descoberta do vírus Stuxnet, seguida da dos vírus Duqu e Flame, anuncia uma nova era de softwares extremamente complexos feitos por Estados poderosos que podem ser utilizados como armas para atacar Estados mais fracos. Sua agressiva utilização no Irã visa a prejudicar as tentativas persas de conquistar a soberania nacional, uma perspectiva condenada pelos interesses norte-americanos e israelenses na região.

Antigamente, o uso de vírus de computador como armas ofensivas não passava de uma trama encontrada em livros de ficção científica. Hoje se trata de uma realidade global, estimulada pelo comportamento temerário da administração Obama, que viola as leis internacionais. Agora, outros Estados seguirão o exemplo, refor-

çando sua capacidade ofensiva como um meio de se proteger. Neste novo e perigoso mundo, o avanço da iniciativa cypherpunk e da construção da ciberpaz é extremamente necessário.

Os Estados Unidos não são os únicos culpados. Nos últimos anos, a infraestrutura da internet de países como a Uganda foi enriquecida pelo investimento chinês direto. Empréstimos substanciais estão sendo distribuídos em troca de contratos africanos com empresas chinesas para construir uma infraestrutura de *backbones* de acesso à internet ligando escolas, ministérios públicos e comunidades ao sistema global de fibras ópticas.

A África está entrando na internet, mas com hardware fornecido por uma aspirante a superpotência estrangeira. Há o risco concreto de a internet africana ser usada para manter a África subjugada no século XXI, e não como a grande libertadora que se acredita que a internet seja. Mais uma vez, a África está se transformando em um palco para os confrontos entre as potências globais dominantes. As lições da Guerra Fria não devem ser esquecidas ou a história se repetirá.

Essas são apenas algumas das importantes maneiras pelas quais a mensagem deste livro vai além da luta pela liberdade individual.

Os cypherpunks originais, meus camaradas, foram em grande parte libertários. Buscamos proteger a liberdade individual da tirania do Estado, e a criptografia foi a nossa arma secreta. Isso era subversivo porque a criptografia era de propriedade exclusiva dos Estados, usada como arma em suas variadas guerras. Criando nosso próprio software contra o Estado e disseminando-o amplamente, liberamos e democratizamos a criptografia, em uma luta verdadeiramente revolucionária, travada nas fronteiras da nova internet. A reação foi rápida e onerosa, e ainda está em curso, mas o gênio saiu da lâmpada.

O movimento cypherpunk, porém, se estendeu além do libertarismo.

Os cypherpunks podem instituir um novo legado na utilização da criptografia por parte dos atores do Estado: um legado para se opor às opressões internacionais e dar poder ao nobre azarão. A criptografia pode proteger tanto as liberdades civis individuais como a soberania e a independência de países inteiros, a solidariedade entre grupos com uma causa em comum e o projeto de emancipação global. Ela pode ser utilizada para combater não apenas a tirania do Estado sobre os indivíduos, mas a tirania do império sobre a colônia. Os cypherpunks exercerão seu papel na construção de um futuro mais justo e humano. É por isso que é importante fortalecer esse movimento global.

Acredito firmemente nessa mensagem, escrita nas entrelinhas deste livro, apesar de não discutida em grandes detalhes. A mensagem merece um livro à parte, do

qual me ocuparei quando chegar o momento certo e minha situação permitir. Por enquanto, espero que baste chamar a atenção para essa questão e pedir que você a mantenha em mente durante a leitura.

Julian Assange
Londres, janeiro de 2013

INTRODUÇÃO
Um chamado à luta criptográfica

Este livro não é um manifesto. Não há tempo para isso. Este livro é um alerta.

O mundo não está deslizando, mas avançando a passos largos na direção de uma nova distopia transnacional. Esse fato não tem sido reconhecido de maneira adequada fora dos círculos de segurança nacional. Antes, tem sido encoberto pelo sigilo, pela complexidade e pela escala. A internet, nossa maior ferramenta de emancipação, está sendo transformada no mais perigoso facilitador do totalitarismo que já vimos. A internet é uma ameaça à civilização humana.

Essas transformações vêm ocorrendo em silêncio, porque aqueles que sabem o que está acontecendo trabalham na indústria da vigilância global e não têm nenhum incentivo para falar abertamente. Se nada for feito, em poucos anos a civilização global se transformará em uma distopia da vigilância pós-moderna, da qual só os mais habilidosos conseguirão escapar. Na verdade, pode ser que isso já esteja acontecendo.

Muitos escritores já refletiram sobre o que a internet significa para a civilização global, mas eles enganaram-se. Enganaram-se porque não têm a perspectiva da experiência direta. Enganaram-se porque nunca se viram cara a cara com o inimigo.

Nenhuma descrição do mundo sobrevive ao primeiro contato com o inimigo.

Nós nos vimos cara a cara com o inimigo.

Ao longo dos seis últimos anos, o WikiLeaks entrou em conflito com praticamente todos os Estados mais poderosos. Conhecemos o novo Estado da vigilância do ponto de vista de um *insider*, porque investigamos seus segredos. Conhecemo-no da perspectiva de um combatente, porque tivemos de proteger nosso pessoal, nossas finanças e nossas fontes de seus ataques. Conhecemo-no de uma perspectiva global, porque temos pessoas, recursos e informações em praticamente todos os países do mundo. Conhecemo-no da perspectiva do tempo, porque temos comba-

tido esse fenômeno há anos e o vimos multiplicar-se e disseminar-se, vez após vez. Trata-se de um parasita invasivo, que engorda à custa de sociedades que mergulham na internet. Ele chafurda pelo planeta, infectando todos os Estados e povos que encontra pela frente.

O que pode ser feito?

Era uma vez, em um lugar que não era nem aqui nem lá, alguns construtores e cidadãos da jovem internet – nós –, que conversaram sobre o futuro do nosso novo mundo.

Vimos que os relacionamentos entre todas as pessoas seriam mediados pelo nosso novo mundo – e que a natureza dos Estados, definida pelo modo como as pessoas trocam informações, valores econômicos e força, também mudaria.

Vimos que a fusão entre as estruturas estatais existentes e a internet criava uma abertura para mudar a natureza dos Estados.

Antes de tudo, lembre-se de que os Estados são sistemas através dos quais fluem as forças repressoras. Facções de um Estado podem competir entre si por apoio, levando ao fenômeno da democracia aparente, mas por trás dessa fachada se encontram, nos Estados, a sistemática aplicação – e fuga – da violência. Posse de terras, propriedades, arrendamentos, dividendos, tributações, multas impostas por decisão judicial, censura, direitos autorais e marcas registradas, tudo isso se faz cumprir por meio da ameaça de aplicação da violência por parte do Estado.

Em geral nem chegamos a nos conscientizar de quão próximos estamos da violência, porque todos nós fazemos concessões para evitá-la. Como marinheiros a favor do vento, raramente percebemos que, abaixo da superfície visível do nosso mundo, se esconde uma grande escuridão.

No novo espaço da internet, qual seria o mediador das forças repressoras?

Será que tem sentido fazer essa pergunta? Nesse espaço sobrenatural, nesse reino aparentemente platônico de ideias e fluxo de informações, será que a noção de forças repressoras conseguiria sobreviver? Será mesmo possível existir uma força capaz de alterar os registros históricos, grampear telefones, separar pessoas, transformar a complexidade em escombros e erigir muros, como um exército de ocupação?

A natureza platônica da internet, das ideias e dos fluxos de informações, é degradada por suas origens físicas. Ela se fundamenta em cabos de fibra óptica que cruzam oceanos, satélites girando sobre nossa cabeça, servidores abrigados em edifícios, de Nova York a Nairóbi. Da mesma forma como o soldado que assassinou Arquimedes com uma simples espada*, uma milícia armada também

* Provável referência a uma das versões da morte do pensador grego Arquimedes (287 a.C.-212 a.C.), segundo a qual ele se encontrava tão absorto em diagramas traçados na areia que não percebeu a invasão romana da cidade de Siracusa e foi assassinado por um soldado. (N. T.)

poderia assumir o controle do auge do desenvolvimento da civilização ocidental, nosso reino platônico.

O novo mundo da internet, abstraído do velho mundo dos átomos concretos, sonhava com a independência. No entanto, os Estados e seus aliados se adiantaram para tomar o controle do nosso novo mundo – controlando suas bases físicas. O Estado, tal qual um exército ao redor de um poço de petróleo ou um agente alfandegário forçando o pagamento de suborno na fronteira, logo aprenderia a alavancar seu domínio sobre o espaço físico para assumir o controle do nosso reino platônico. O Estado impediria nossa tão sonhada independência e, imiscuindo-se pelos cabos de fibra óptica, pelas estações terrestres e pelos satélites, iria ainda mais longe, interceptando em massa o fluxo de informações do nosso novo mundo – a sua própria essência –, ao mesmo tempo que todos os relacionamentos humanos, econômicos e políticos o receberiam de braços abertos. O Estado se agarraria como uma sanguessuga às veias e artérias das nossas novas sociedades, engolindo sofregamente todo relacionamento expresso ou comunicado, toda página lida na internet, todo e-mail enviado e todo pensamento buscado no Google, armazenando esse conhecimento, bilhões de interceptações por dia, um poder inimaginável, para sempre, em enormes depósitos ultrassecretos. E passaria a minerar incontáveis vezes esse tesouro, o produto intelectual privado coletivo da humanidade, com algoritmos de busca de padrões cada vez mais sofisticados, enriquecendo o tesouro e maximizando o desequilíbrio de poder entre os interceptores e um mundo inteiro de interceptados. E, então, o Estado ainda refletiria o que aprendeu de volta ao mundo físico, para iniciar guerras, programar *drones**, manipular comitês das Nações Unidas e acordos comerciais e realizar favores à sua ampla rede de indústrias, *insiders* e capangas conectados.

Mas nós fizemos uma descoberta. Nossa única esperança contra o domínio total. Uma esperança que, com coragem, discernimento e solidariedade, poderíamos usar para resistir. Uma estranha propriedade do universo físico no qual vivemos.

O universo acredita na criptografia.

É mais fácil criptografar informações do que descriptografá-las.

Notamos que seria possível utilizar essa estranha propriedade para criar as leis de um novo mundo. Para abstrair nosso novo reino platônico de sua base composta de satélites, de cabos submarinos e de seus controladores. Para fortalecer nosso espaço por trás de um véu criptográfico. Para criar novos espaços fechados àqueles que controlam a realidade física, porque a tarefa de nos seguir nesses lugares demandaria recursos infinitos.

E, assim, declarar a independência.

---

* Tipo de veículo aéreo de combate não tripulado. (N. T.)

Os cientistas do Projeto Manhattan descobriram que o universo permitia a construção de uma bomba nuclear. Essa não foi uma conclusão óbvia. Talvez as armas nucleares não estivessem dentro das leis da física. No entanto, o universo acredita em bombas atômicas e reatores nucleares. Eles são um fenômeno abençoado pelo universo, como o sal, o mar ou as estrelas.

De maneira similar, o universo, o nosso universo físico, apresenta essa propriedade que possibilita que um indivíduo ou um grupo de indivíduos codifique algo de maneira confiável, automática e até inconsciente, de forma que nem todos os recursos e nem toda a vontade política da mais forte superpotência da Terra será capaz de decifrá-lo. E as trajetórias de criptografia entre as pessoas podem se fundir para criar regiões livres das forças repressoras do Estado externo. Livres da interceptação em massa. Livres do controle do Estado.

Desse modo, as pessoas poderão se opor a uma superpotência plenamente mobilizada e vencer. A criptografia é uma incorporação das leis da física e não se deixa abalar pela petulância dos Estados nem pelas distopias da vigilância transnacional.

Não está claro se o mundo terá de ser realmente assim. Mas, de uma forma ou de outra, o universo recebe a criptografia de braços abertos.

A criptografia é a derradeira forma de ação direta não violenta.

Enquanto Estados munidos de armas nucleares podem impor uma violência sem limites a milhões de indivíduos, uma criptografia robusta significa que um Estado, mesmo exercendo tal violência ilimitada, não tem como violar a determinação de indivíduos de manter segredos inacessíveis a ele.

Uma criptografia robusta é capaz de resistir a uma aplicação ilimitada de violência. Nenhuma força repressora poderá resolver uma equação matemática.

Mas será que poderíamos pegar esse fato estranho sobre o mundo e amplificá-lo para que ele atue como um elemento constitutivo emancipatório básico para a independência da humanidade no reino platônico da internet? E, à medida que as sociedades mergulham na internet, será que essa liberdade poderia se refletir de volta na realidade física, a fim de redefinir o Estado?

Lembre-se de que os Estados são os sistemas que decidem onde e como as forças repressoras são sistematicamente aplicadas.

A questão de até que ponto as forças repressoras vindas do mundo físico podem se infiltrar no reino platônico da internet é respondida pela criptografia e pelos ideais dos cypherpunks.

À medida que os Estados se fundem com a internet e o futuro da nossa civilização se transforma no futuro da internet, devemos redefinir as relações de força.

Se não o fizermos, a universalidade da internet se fundirá com a humanidade global em uma gigantesca grade de vigilância e controle em massa.

É preciso acionar o alarme. Este livro é o grito de advertência de uma sentinela na calada da noite.

No dia 20 de março de 2012, em prisão domiciliar no Reino Unido e aguardando a extradição, encontrei-me com três amigos e colegas sentinelas na esperança de que, em uníssono, nossa voz possa despertar a cidade. Precisamos transmitir o que aprendemos enquanto você, leitor, ainda tem uma chance de entender o que está acontecendo e fazer alguma coisa a respeito.

É chegada a hora de pegar as armas deste nosso novo mundo, para lutar por nós mesmos e por aqueles que amamos.

Nossa missão é proteger a autodeterminação onde for possível, impedir o avanço da distopia onde não for possível e, se tudo mais falhar, acelerar sua autodestruição.

Julian Assange
Londres, outubro de 2012

Julian Assange

Jérémie Zimmermann









Jacob Appelbaum

Andy Müller-Maguhn

Os autores

Julian Assange é o editor-chefe e visionário por trás do WikiLeaks[1]. Um dos contribuintes originais da lista de discussão Cypherpunk, hoje é um dos maiores expoentes dessa filosofia no mundo. Seu trabalho com o WikiLeaks conferiu força política à justaposição tradicional dos cypherpunks: “Privacidade para os fracos, transparência para os poderosos”. Apesar de seu trabalho mais visível envolver o vigoroso exercício da liberdade de expressão para forçar a transparência e a prestação de contas por parte de poderosas instituições, ele é um grande crítico da invasão da privacidade de indivíduos por parte do Estado e das corporações. Julian também é autor de inúmeros projetos de software alinhados à filosofia cypherpunk, como o strobe.c, o primeiro *scanner* de portas TCP/IP, o arquivo *rubberhose** de criptografia negável [*deniable encryption*] e o código original do WikiLeaks[2]. Na adolescência, Julian pesquisava segurança de rede e computação antes de algumas modalidades de *hacking* serem consideradas atividades criminais por lei. Nos anos 1990, Julian tornou-se ativista e criou o próprio provedor de acesso à internet na Austrália. Com Sulette Dreyfus, é coautor de um livro sobre a história do movimento *hacker* internacional, intitulado *Underground*, que inspirou o filme *Underground*: *the Julian Assange Story*[3].

Jacob Appelbaum é um dos fundadores da Noisebridge, em São Francisco, membro do Chaos Computer Club de Berlim e desenvolvedor de softwares[4].

* O *rubberhose* é uma espécie de pacote de criptografia negável (criptografia com chaves falsas que produzem mensagens falsas supostamente decifradas) que criptografa dados, com transparência, em um dispositivo de armazenamento, como um disco rígido, permitindo que o usuário oculte parte desses dados criptografados. (N. T.)

Também é um defensor e pesquisador do Tor Project, sistema on-line anônimo que possibilita às pessoas resistir à vigilância e contornar a censura na internet[5]. Na última década ele se concentrou em ajudar ativistas em defesa do meio ambiente e dos direitos humanos. Com esse objetivo, publicou pesquisas originais relativas a segurança, privacidade e anonimato em uma ampla variedade de áreas, da computação forense ao uso medicinal da maconha. Jacob acredita que todas as pessoas têm o direito de ler sem restrições e o direito de se expressar livremente, sem exceções. Em 2010, quando Julian Assange foi impossibilitado de proferir uma palestra em Nova York, Jacob a assumiu em seu lugar. Desde então, ele, seus amigos e seus parentes têm sido perseguidos pelo governo dos Estados Unidos. Foi interrogado em aeroportos, submetido a revistas invasivas e intimidado por oficiais de órgãos de manutenção da ordem pública com ameaças veladas de estupro na prisão, além de ter seus equipamentos confiscados e seus serviços on-line sujeitos a uma intimação judicial secreta. Jacob não se deixa abalar por essas medidas, continua a combater essas questões legais e permanece um vigoroso defensor da liberdade de expressão e do WikiLeaks.

Andy Müller-Maguhn é membro de longa data do Chaos Computer Club, na Alemanha, além de ex-membro do conselho e porta-voz da organização[6]. Foi cofundador da European Digital Rights (Edri), ONG que defende a garantia dos direitos humanos na era digital[7]. De 2000 a 2003, foi eleito por usuários europeus de internet para atuar como diretor europeu da Internet Corporation for Assigned Names and Numbers [Corporação da Internet para Atribuição de Nomes e Números] (Icann), responsável pela elaboração de políticas internacionais para a determinação de "nomes e números" na internet*[8]. É especialista em telecomunicações e vigilância e se dedica a investigar a indústria da vigilância com seu projeto wiki, o Buggedplanet.info[9]. Andy trabalha com comunicações criptográficas e ajudou a criar uma empresa chamada Cryptophone, que comercializa dispositivos de comunicação vocal segura para clientes comerciais e presta consultoria estratégica em arquitetura de redes[10].

Jérémie Zimmermann é cofundador e porta-voz do grupo de apoio aos cidadãos La Quadrature du Net, a mais proeminente organização europeia em defesa

* Segundo a filial brasileira da organização, "a Icann é responsável pela coordenação global do sistema de identificadores exclusivos da internet. Entre esses identificadores estão nomes de domínio (como .org, .museum e códigos de países, como .uk) e endereços usados em vários protocolos da internet. Os computadores usam esses identificadores para se comunicar entre si pela internet", disponível em: <www.icann.org.br>. (N. T.)

do direito do anonimato on-line e na promoção da conscientização das pessoas sobre os ataques legislativos à liberdade na internet[11]. Dedica-se a criar ferramentas para que as pessoas possam tomar parte em debates públicos e tentar realizar mudanças. Atualmente se encontra profundamente envolvido com questões relativas à guerra de direitos autorais, com o debate sobre a neutralidade da rede e outras questões legislativas fundamentais para o futuro de uma internet livre. Recentemente o grupo La Quadrature du Net conquistou uma vitória histórica na política europeia, organizando uma campanha pública para derrotar o Acta (Anti-Counterfeiting Trade Agreement [Acordo Comercial Antifalsificação]) no Parlamento Europeu. Logo depois de participar da conversa que constitui as bases deste livro, Jérémie foi detido por dois oficiais do FBI ao sair dos Estados Unidos e interrogado sobre o WikiLeaks.

Notas

1 WikiLeaks: <http://wikileaks.org>.

2 Para mais informações sobre os arquivos *rubberhose*, ver Suelette Dreyfus, *The Idiot Savants' Guide to Rubberhose*, disponível em: <http://marutukku.org/current/src/doc/maruguide/t1.html>. Acesso em 14 out. 2012.

3 Sobre o livro *Underground*, ver <http://www.underground-book.net>. Quanto ao filme *Underground: the Julian Assange Story*, ver Internet Movie Database, em: <http://www.imdb.com/title/tt2357453/>. Acesso em 21 out. 2012.

4 A Noisebridge [literalmente, "ponte do barulho", em inglês] é um *hackerspace* de São Francisco que fornece infraestrutura para projetos técnicos criativos e é operado de forma colaborativa. Ver: <www.noisebridge.net/wiki/Noisebridge>. O Chaos Computer Club Berlin é o braço berlinense do Chaos Computer Club (ver nota 6): <https://berlin.ccc.de/wiki/Chaos_Computer_Club_Berlin>.

5 Tor Project: <www.torproject.org>.

6 O Chaos Computer Club é a maior associação de *hackers* da Europa. Suas atividades variam de investigação e pesquisa técnica a campanhas, eventos, publicações e consultoria política: <www.ccc.de>.

7 European Digital Rights: <http://www.edri.org>.

8 Internet Corporation for Assigned Names and Numbers: <www.icann.org>.

9 Buggedplanet: <http://buggedplanet.info>.

10 Cryptophone: <www.cryptophone.de>.

11 La Quadrature du Net: <www.laquadrature.net>.